GLOBAL DEFENSE, INC.

STEALTH AND DECEPTION – SPEED AND VIOLENCE:

How the New Threat Affects Physical Protection Systems

Global Defense, Inc.

Brian Sanford, President, GDI

Tim Ryan, Assistant Director of Operations, GDI

Global Defense, Inc.

This briefing is:

UNCLASSIFIED

Thesis

- High-risk facilities should re-evaluate their Physical Protection Systems (PPS) based on terrorists' current Method of Operation.

Current Method of Operation (MO)

- Stealth and Deception
  - Position Terrorists and Assets for attack
  - At Detection, or time of the their choosing, strategy shifts
- Speed and Violence
  - Multiple, synchronized Improvised Explosive Devices (IEDs)
  - Detonated at self-lethal range

Old Physical Protection Systems

- Designed prior to realistic terrorist threat on American soil
- Focused on deterrence of vandalism, theft

New Physical Protection System

- Developed by Sandia National Laboratories
- Well-established methodology used to protect nuclear assets
- Concepts are not “new”, but application to non-nuclear, high-risk facilities is a current trend

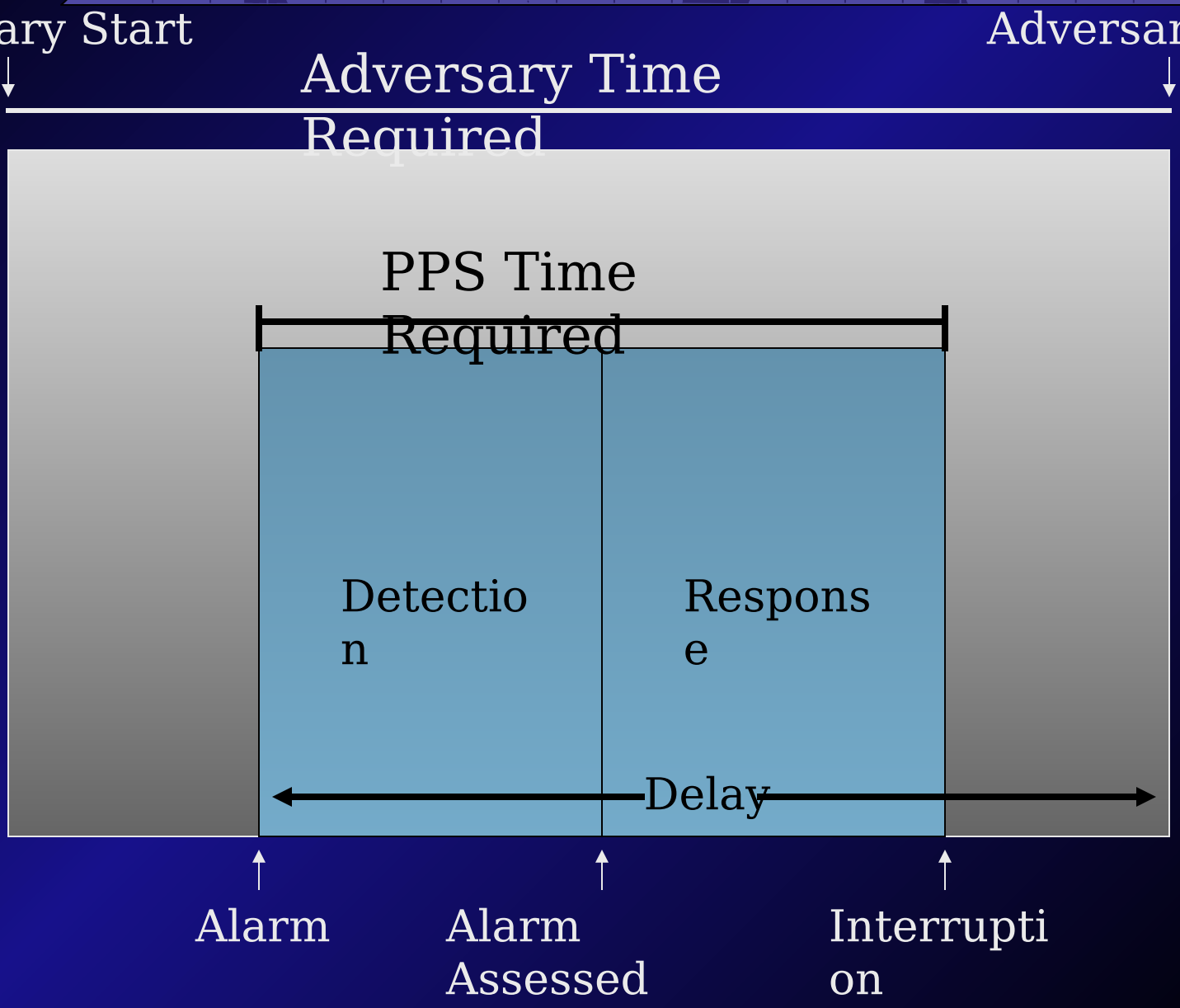
Assumptions Challenged

- Application of Sandia model must consider new threat
- By using Stealth and Deception, Detection/Assessment may not occur at the perimeter
- By using Speed and Violence in a suicidal manner, time available to defeat an attack is significantly reduced

PPS Functions Review

- Detection (useless without assessment)
  - Perimeter and entry control most common
- Delay (multiple, serial barriers)
  - provide time for response force to arrive and interrupt the adversary
- Response – clear communication essential
  - Must have capability to interrupt adversary prior to mission accomplishment

GLOBAL DEFENSE, INC.



Graph

PPS Characteristics Review

- Balanced Protection
  - Equal time and difficulty along all possible paths
- Protection –In – Depth
  - multiple obstacles that must be defeated in sequence
- Redundancy
  - mitigates the danger of individual component degradation

Design Basis Threat (DBT)

- The DBT is the worst potential adversary or scenario that a facility's PPS is created to defeat
- Nuclear facilities have used the following DBT
  - The DBT is considered to include an attack using stealth and deception initially, then a determined, violent assault by several persons who may be well trained, have inside assistance, weapons, tools, vehicles, and the ability to operate as two or more teams

"Containment" vs. "Denial"

- Suicidal terrorists do not need to escape to succeed
- This reduces the time available to intervene
- "Containment" strategy previously used
  - Adversary could "get-in", but response force would arrive before they could "get-out"
- "Denial" strategy more appropriate
  - Terrorists must be interrupted prior to reaching critical node.

Even Less Time Available

- Using Stealth and Deception, detection may not occur at the perimeter
- Adversary time spent before detection does not “count”.
- Highlights the importance of Delay and Response
- U.S.S. Cole attack

"Swipe-card" Example

- Expands a secure perimeter to each cardholder's purse, vehicle, or home.
- To defeat a secure perimeter at a hardened facility, terrorist need only break in to an employee's car
- He may enter undetected, and have a considerable "head-start" on the response force once he is detected

Critical Detection Point (CDP)

- The CDP is any position on a facility where if an adversary is detected, there is enough time remaining for the response force to interrupt the adversary

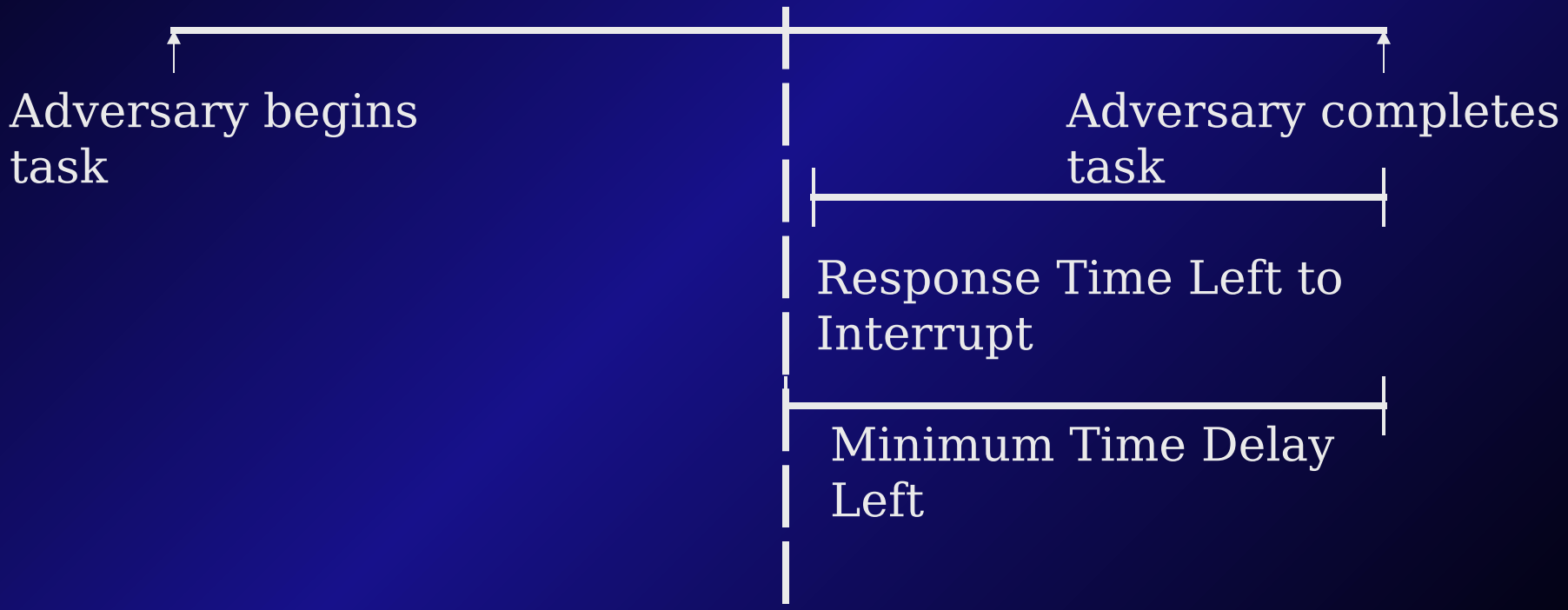
GLOBAL DEFENSE, INC.

STEALTH AND DECEPTION

Adversary Minimizes Detection

SPEED AND VIOLENCE

Adversary Minimizes Delay



Critical Detection Point:

Minimum delay along terrorists' path just exceeds the response force's time to interrupt

Graph

CDP Failings

- Many facilities do not know where their CDP is
- If they do know, they assume that detection will occur at the perimeter
- Many perimeters are built on property lines, without regard to their CDP.
- In many cases, the CDP might already be OUTSIDE of the perimeter

Speed and Violence

- Adversary may completely disregard stealth and still accomplish his mission.
- Beyond the Critical Detection Point at the beginning of the attack
- Demonstrated just last month in Riyadh, Saudi Arabia.
  - Terrorists shot armed guards, and took less than one minute to detonate three IEDs at Western housing complexes

Response Force Limitations

- Response force may not be adequate, or have adequate information to stop violent adversaries
- Columbine example
  - Officers on scene in minutes.
  - Took over one hour AFTER adversaries' suicides for officers to enter building
  - First responders cautious due to unknown threat

Response Force Limitations (cont)

- Response force caution can be expected
  - So many first responders died on September 11th when the World Trade Center Towers collapsed
  - Potential threat of Nuclear, Biological, or Chemical (NBC) contaminants in a future terrorist attack
- Undue caution minimized with clear, concise, and consistent communications
- Practice the communication and security plan with the response force and local law enforcement

Conclusions

- "Bombings are responsible for approximately 70 percent of the historical occurrences of terrorist activity."
- Deterrence is no longer sufficient
  - The absence of an attack does not validate a facility's current Physical Protection System
- High-Risk facilities must seek expertise on PPS design

Conclusions (continued)

- Delay is too often neglected
- CDP must be determined
- Practice drills with law enforcement and medical responders and simulated “terrorists” must be conducted and evaluated regularly
- Follow through with lessons learned. Facilities must adjust their CDP and PPS accordingly

Summary

- Terrorists are not afraid of dying, they are afraid of failing
- They will develop plans that have the greatest impact and probability of success
- By employing tactics of Stealth and Deception, detection may not occur at the perimeter.

Summary (continued)

- By employing tactics of Speed and Violence, security may be evacuating instead of responding
- High-risk facilities must re-evaluate their Physical Protection Systems in light of sound PPS design criteria, current intelligence, and adversary methods.

Questions?